PCT/JP2004/006288

30.4.2004

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application:	２００３年　５月　９日
出願番号 Application Number:	特願２００３－１３１３７２
[ST. 10/C] :	[ＪＰ２００３－１３１３７２]
出願人 Applicant(s):	松下電器産業株式会社

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

２００４年　６月１０日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００４－３０５００９０

【書類名】　特許願

【整理番号】　2022550173

【特記事項】　特許法第３６条の２第１項の規定による特許出願

【提出日】　平成15年 5月 9日

【あて先】　特許庁長官殿

【国際特許分類】　H04K 1/00

【発明者】

【住所又は居所】　シンガポール５３４４１５シンガポール、タイ・セン・アベニュー、ブロック１０２２、０４－３５３０番、タイ・セン・インダストリアル・エステイト、パナソニック・シンガポール研究所株式会社内

【氏名】　ジ・ミン

【発明者】

【住所又は居所】　シンガポール５３４４１５シンガポール、タイ・セン・アベニュー、ブロック１０２２、０４－３５３０番、タイ・セン・インダストリアル・エステイト、パナソニック・シンガポール研究所株式会社内

【氏名】　リュウ・ジン

【発明者】

【住所又は居所】　シンガポール５３４４１５シンガポール、タイ・セン・アベニュー、ブロック１０２２、０４－３５３０番、タイ・セン・インダストリアル・エステイト、パナソニック・シンガポール研究所株式会社内

【氏名】　シェン　メイ・シェン

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　妹尾　孝憲

【特許出願人】

【識別番号】　000005821

【住所又は居所】　大阪府門真市大字門真１００６番地

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100086405

【弁理士】

【氏名又は名称】　河宮　治

【選任した代理人】

【識別番号】　100098280

【弁理士】

【氏名又は名称】　石野　正弘

【手数料の表示】

【予納台帳番号】　163028

【納付金額】　35,000円

【提出物件の目録】

【物件名】　外国語明細書　1

【物件名】　外国語図面　1

【物件名】　外国語要約書　1

【包括委任状番号】　9602660

【プルーフの要否】　要

【書類名】　外国語明細書

1 TITLE OF THE INVENTION

Apparatus of a flexible protection of ISMA media streams using MPEG-4 IPMP Extension

2 WHAT IS CLAIMED IS:

(1) Apparatus of a flexible protection of ISMA media streams using MPEG-4 IPMP Extension, on ISMA content provider side, comprising the following steps of:

Embed Tool List Descriptor into IOD to indicate a list of IPMP tools required to process the content.

One of the tools specified in the Tool List has a tool ID which was assigned to ISMACryp decryption tool.

One of the tools specified in the Tool List has a tool ID which was assigned to KMS (Key Management System) tool.

Presence of any one of the above mentioned two tools signals the presence of ISMACryp protection.

(2) Apparatus of a flexible protection of ISMA media streams using MPEG-4 IPMP Extension, on ISMA content provider side, where signalling ISMACryp protection using Tool List in IOD in claim (1), further comprising the following steps of:

Embed IPMP Descriptor Pointer in the ES Descriptor of a media stream to indicate the media stream is protected.

The IPMP Descriptor referenced by the above said IPMP Descriptor Pointer has a tool ID of the ISMACryp decryption tool.

(3) Apparatus of a flexible protection of ISMA media streams using MPEG-4 IPMP Extension, on ISMA content provider side, comprising the following steps of:

Carry ISMACryp parameters in ISMACryp_Data which extends from IPMP_Data_BaseClass.

Carry ISMACryp_Data in IPMP Descriptor which is subsequently carried in OD.

(4) Apparatus of a flexible protection of ISMA media streams using MPEG-4 IPMP Extension, on ISMA content provider side, comprising the following steps of:

Carry ISMACryp parameters in ISMACryp_Data which extends from IPMP_Data_BaseClass.

Carry ISMACryp_Data in IPMP_Message which is subsequently carried in IPMP Stream.

3 DETAILED DESCRIPTION OF THE INVENTION

3.1 Industrial Field of Utilization

The presented invention aims to provide MPEG-4 IPMP Extension compatible extension to the ISMA protection framework. With the given invention adopted, ISMA protection framework is able to achieve interoperability with MPEG-4 IPMP Extension compatible receivers.

3.2 Background and Prior Art

For several years, the promise of delivering video and audio over the Internet has been widely promoted in the media content distribution industry. Many standard groups have put tremendous efforts to provide solutions towards this issue. Internet Streaming Media Alliance (ISMA) is one of such groups. It addresses this need by setting forth a framework for the use of existing open standards that vendors can use to build interoperable video and audio systems for use in IP framework and Internet. Its specification assumes the use of existing MPEG technologies and mainly focus on MPEG-4 technologies at the current stage, though future adaptation and revisions may include MPEG-2 and MPEG-7 technologies.

ISMA also defines a cryptographic framework, namely ISMACryp, for ISMA media streams. This framework is extensible to new media encodings, can be upgraded to new cryptographic transforms, and is applicable to a variety of key management, security, or digital rights management (DRM)) systems. It also defines a default encryption of media streams and authentication of media messages for ISMA specification. Figure.1 gives the architecture diagram of ISMACrpt protection over the ISMA framework.

As ISMA declares, two types of receivers are targeted, namely, ISMA-only receivers and MPEG system-capable receivers. "ISMA-only" receivers are defined here as receivers that are not MPEG-4 system capable, i.e., cannot process the MPEG-4 signalling and control (elementary) streams that can accompany any MPEG-4 (elementary) media stream. On the contrary, "MPEG system-capable receivers" can process the MPEG-4 systems layer information as well as ISMA related information. The interoperability with MPEG system-capable receivers is achieved through MPEG IOD (Initial Object Description) that conveys at least a minimal level of MPEG-system signalling. The IOD is included as a binary SDP (Session Description Protocol) attribute, i.e., SDP IOD.

ISMACryp is also applicable to both types of receivers. It extends the binary IOD inside the SDP message. The new signalling offers an asymmetry rather than the redundancy found in ISMA signalling: It provides "Minimal" and "Base" signalling parameters of the SDP IOD to maximizes receiver interoperability with MPEG-4 IPMP system.

However, the current ISMACryp defined extension to IOD is not complete and not consistent with latest MPEG-4 IPMP Extension standard. This results the ISMA streams may not be correctly recognizable by MPEG-4 IPMP Extension compatible receiver. For example, ISMACryp standard defines that the presence of IPMP_Descriptor in IOD is used to signal the ISMACryp protection. However according to MPEG-4 IPMP extension, the Tool List Descriptor should be presented in the IOD if there is IPMP protection. These incompleteness and inconsistencies may impair the ISMA framework's interoperability with MPEG-4 IPMP Extension compatible receivers.

3.3 Problem to be solved

This invention tries to solve the following problems:

ISMACryp standard defines the signalling of ISMACryp protection by using MPEG-4 IPMP through the extension of IOD inside SDP. The presence of IPMP_Descriptor in IOD signals the receivers that this media stream is protected. For MPEG IPMP non-compatible receiver, they are then allowed to handle the streams in their proprietary yet appropriate ways, e.g., simply ignore the streams. However, MPEG-4 IPMP Extension standard defines that the Tool List Descriptor should be presented in the IOD to indicate IPMP protection. The standard doesn't guarantee the existence of IPMP_Descriptor in IOD for IPMP protection. Thus, the ISMACryp defined signalling method may not detect the protection mechanism of media streams correctly whose IOD has Tool List descriptor but no IPMP_Descriptor.

Furthermore, in order to enable MPEG-4 IPMP Extension compatible receivers to receive ISMA related data, e.g., encryption information, KMS configuration, which accompany the IPMP data. ISMACryp standard extends the IPMP_Descriptor in IOD with a self-defined ISMACryp_Descriptor based on the MPEG-4 IPMP standard. However, because of the fast evolvement of MPEG-4 IPMP standard, the syntax of IOD has changed and been different with the old version that ISMACryp standard based on. This brings the problem that the ISMA related data carried in IPMP context might not be recognizable by receivers compatible with latest MPEG-4 IPMP Extension standard. In order to keep consistency of latest MPEG-4 IPMP Extension standard while minimizes the changes to ISMA already defined parameters, there requires a new mechanism that is able to carry ISMA related data with current MPEG-4 IPMP Extension standard and the mechanism is backward compatible with previous version of MPEG-4 IPMP Extension standard.

3.4 Means of Solving the Problems

To address the signalling problems, this invention defines a signalling mechanism to signal the presence of ISMACryp protection in MPEG Initial Object Descriptor (IOD). The tool list and IPMP Descriptors are utilized to signal the protection. This means is compatible with the latest MPEG-4 IPMP Extension standard, meanwhile provides maximum interoperability with MPEG-system-capable ISMA receiver. It also provides a flexible way to identify tools required to play the content.

This invention also defines the mechanisms of carrying and converting ISMACryp parameters to MPEG-system-capable ISMA receiver. An ISMA specific ISMACryp_Data can be extended from the MPEG-4 IPMP Extension defined IPMP_Data_BaseClass to carry the ISMACryp parameters. This ISMACryp_Data can then be carried in IPMP Descriptor or IPMP Stream in order to conform to MPEG-4 IPMP Extension standard.

3.5 Operation of the Invention

Within ISMA framework, IOD and OD are constructed. IPMP Tool List Descriptors are embedded into IOD, and IPMP Descriptor Pointers and IPMP Descriptors are embedded into IOD and OD if there is ISMACryp protection present.

The IOD and OD are conveyed to the ISMA receiver that understands MPEG-4 system via SDP IOD signaling. The receiver analyzes IOD and OD. Upon detection of IPMP Tool List, the receiver is aware that there is ISMACryp protection present. Upon detection of IPMP Descriptor Pointer and IPMP Descriptor, the receiver can be aware of which stream is protected by which tool.

Within ISMA framework, when a stream is protected by ISMACryp, the ISMACryp parameters (for example, cipher identifier) can be carried in ISMACryp_Data and put in IPMP Descriptor or IPMP Stream, the carriage of the parameters is MPEG-4 IPMP Extension compliant.

At the receiver side, the parameters for ISMACryp can be retrieved from IPMP Descriptor or IPMP stream in a MPEG-4 IPMP Extension compatible way. The parameters can then be used to configure ISMACryp decryption tool.

3.6 Embodiments

3.6.1 IPMP Extension Signaling

The current ISMACryp supports SDP IOD signaling for ISMA-only and MPEG receivers. ISMA-only receivers accept only SDP FMTP signaling parameters but the SDP IOD must signal any MPEG receiver that the stream has ISMACryp protections (Minimal IPMP signaling). The KMS MAY signal the ISMACryp signaling using only IPMP signaling in the SDP IOD (Base IPMP signaling).

The present document provides the syntax that is compatible with MPEG-4 IPMP Extensions. With minimum effort, ISMACryp can easily achieve compatibility with MPEG-4 IPMP Extension, which provides a more flexible protection scheme.

Minimal IPMP-X Signaling

IPMP Extension defines an IPMP Tool List Descriptor in IOD, which identify a list of required IPMP Tools in following procession. . According to MPEG-4 IPMP extension, the Tool List Descriptor should be presented in the IOD if there is IPMP protection. So for the minimal IPMP-X Signaling, we suggest to use IPMP Tool List Descriptor in IOD instead of the IPMP Descriptor to achieve this purpose.

According to the current ISMACryp specification, which specifies the encryption and KMS information transportation, at least two tools should be presented in the MPEG IPMP Tool List Descriptor. The first one is the KMS tool, and the other is the ISMA decryption tool. The presence of ISMACryp tool in MPEG IPMP Tool List signals the ISMACryp protection.

An example of the Tool List Descriptor with ISMACryp tools is given below.

	IPMP_ToolListDescriptor		
1	8	IPMP_ToolListDescTag	0x60
2	16	Descriptor size	
		IPMP_Tool	
3	8	IPMP_ToolTag	0x61
4	16	Descriptor size	
5	128	IPMP_ToolID	The value assigned by each service provider to their KMS tool
6	1	isAltGroup	0
7	1	isParametric	0
8	6	reserved	0b0000.00
9	8	Size of the tool URL	
10		Tool URL	
		IPMP_Tool	
11	8	IPMP_ToolTag	0x61
12	16	Descriptor size	
13	128	IPMP_ToolID	The value assigned to the ISMA decryption tool
14	1	isAltGroup	0
15	1	isParametric	0

16	6	reserved	0b0000.00
17	8	Size of the tool URL	
18		Tool URL	

IPMP Tool List is depicted in MPEG-4 IPMP Extension content structure shown in Figure 2. Using IPMP Tool List (2.1) not only facilitates the signaling of the presence of ISMACryp protection, but also allows a great flexibility of identifying tools. An IPMP tool in the tool list can be identified in three ways. The first is to use a fixed 128 bit IPMP_ToolID (2.2), value assigned by a registration authority. The second is to use a list of IPMP_ToolIDs to indicate the Tools that are equivalent alternatives to each other (2.3). By doing so, a terminal can have more flexibility to choose its own tool. The last one is to use to parametric description to describe a criteria that an IPMP tool has to meet (2.4), in this case, a terminal can have more freedom to choose a tool to perform the required function.

Base IPMP-X Signaling

For the MPEG-systems-capable receiver, more IPMP information is required for IPMP related processing. The following IPMP-X signaling SHOULD be adopted as the basis for a more capable MPEG IPMP Extension signaling. Together with the Tool List introduced in section 2, they provide the base information required by the MPEG compatible receiver. For encrypted elementary streams, their corresponding ES descriptors MUST contain the following IPMP_DescriptorPointer:

Descriptor Name			
Field No.	Size in Bits	Field Name	Value
			IPMP_DescriptorPointer
1	8	IPMP_DescriptorPointer tag	10
2	8	descriptor size	5
3	8	IPMP_DescriptorID	0xFF
4	16	IPMPX_DescriptorID	0x0002 / 0x0003
5	16	IPMP_ES_ID	0x0000

The concept of this IPMP Extension protection signaling is shown in Figure 3. The presence of this descriptor pointer (3.1 and 3.2) in an ES_Descriptor indicates that the stream associated with this descriptor is subject to protection and management by the IPMP Tool specified in the referenced IPMP_Descriptor (3.3 and 3.4). This referenced IPMP_Descriptor should be carried in the Object Descriptor.

Descriptor Name			
Field No.	Size in Bits	Field Name	Value
		IPMP_Descriptor	
1	8	IPMP_Descriptor tag	11
2	8	descriptor size	23

3	8	IPMP_DescriptorID	0xFF
4	16	IPMPS_Type	0xFFFF
5	16	IPMP_DescriptorIDEx	0x0002 / 0x0003
6	128	IPMP_ToolID	The value assigned to the ISMA decryption tool
7	8	ControlPointCode	0x01 (between the decode buffer and the decoder)
8	8	SequenceCode	0x80

Also, the IOD must contain the following IPMP_DescriptorPointer. In the following example, it tells that the specific DRM tool (Key Management System) indicated in the referenced descriptor must be instantiated at a global scope:

Descriptor Name			
Field No.	Size in Bits	Field Name	Value
		IPMP_DescriptorPointer	
1	8	IPMP_DescriptorPointer tag	10
2	8	descriptor size	5
3	8	IPMP_DescriptorID	0xFF
4	16	IPMP_DescriptorIDEx	0x0001
5	16	IPMP_ES_ID	0x0000

The above IPMP_DescriptorPointer points to a IPMP_Descriptor whose IPMP_DescriptorIDEx is 0x0001. Then the specified IPMP_Descriptor must be presented in IOD. Note for the KMS, the descriptor’s s controlPoint should be set to 0x00 to indicate a global scope.

Descriptor Name			
Field No.	Size in Bits	Field Name	Value
		IPMP_Descriptor	
1	8	IPMP_Descriptor tag	11
2	8	descriptor size	22
3	8	IPMP_DescriptorID	0xFF
4	16	IPMPS_Type	0xFFFF
5	16	IPMP_DescriptorIDEx	0x0001
6	128	IPMP_ToolID	The value assigned by each service provider to their KSM tool
7	8	ControlPointCode	0x00 (no control point)

3.6.2 Carriage of ISMACryp data in an IPMP Extension compatible way

ISMACryp uses a set of parameters to describe the encryption of the streams. In order to carry parameters carried in an IPMP Extension compatible way, an ISMACryp_Data can be extended from the IPMP-X defined IPMP_Data_BaseClass. IPMP_Data_BaseClass is defined in MPEG-4 IPMPX as shown below:

```
abstract aligned(8) expandable(2^28-1) class IPMP_Data_BaseClass:
  bit(8) tag=0 .. 255
{
  bit(8)  Version;
  bit(32) dataID;
  // Fields and data extending this message.
}
```

ISMACryp_Data can extend from the above base class using a user-defined tag. The data can then have its own set of fields to carry the parameters. This can ensure interoperability of different ISMA terminals interpreting the same content stream.

This ISMACryp_Data can be carried in two places in a standard way. The first is to carry it in IPMP Descriptor. The example of an IPMP Descriptor with this ISMACryp_Data is shown below:

Descriptor Name			
Field No.	Size in Bits	Field Name	Value
		IPMP_Descriptor	
1	8	IPMP_Descriptor tag	11
2	8	descriptor size	23
3	8	IPMP_DescriptorID	0xFF
4	16	IPMPS_Type	0xFFFF
5	16	IPMP_DescriptorIDEx	0x0002 / 0x0003
6	128	IPMP_ToolID	The value assigned to the ISMA decryption tool
7	8	ControlPointCode	0x01 (between the decode buffer and the decoder)
8	8	SequenceCode	0x80
		ISMACryp_Data	
7	8	ISMACryp_DataTag	to be defined
8	8	data size	20
9	8	Cipher-suite	Cipher identifier
11	4	IV-length	Byte length of the initialization vector
12	2	Delta-IV-length	Byte length of the IV on an AU basis
13	1	Selective-encryption	1 if selective encryption is used
14	1	Key-indicator-per-Au	1 if multiple key indicators appear in a packet
15	8	Key-indicator-length	Byte length of the key indicator

The second way to carry the ISMACryp_Data is to carry it as a payload in IPMP_Message which is subsequently carried in IPMP Stream as defined in MPEG-4 IPMP Extension.

```
aligned(8) expandable(2^28-1) class IPMP_Message
{
  bit(16)  IPMPS_Type;
  if (IPMPS_Type == 0)
  {
    bit(8) URLString[sizeOfInstance-2];
  }
  else (if (IPMPS_Type == 0x0001)
  {
    bit(16) IPMP_DescriptorID;
       IPMP_Data_BaseClass IPMP_ExtendedData[]
  } else {
    bit(8) IPMP_data[sizeOfInstance-2];
  }
}
```

The following example shows the syntax of the IPMP_Message when it carries ISMACryp_Data, The IPMP tool specified in the IPMP Descriptor with this IPMP_DescriptorIDEx is the destination of the IPMP_Message.

Field No.	Size in Bits	Field Name	Value
		IPMP_Message	
1	16	message size	
2	16	IPMPS_Type	0x0001
3	16	IPMP_DescriptorIDEx	
		ISMACryp_Data	
4	8	ISMACryp_DataTag	to be defined
5	8	data size	20
6	8	Cipher-suite	Cipher identifier
7	4	IV-length	Byte length of the initialization vector
8	2	Delta-IV-length	Byte length of the IV on an AU basis
9	1	Selective-encryption	1 if selective encryption is used
10	1	Key-indicator-per-Au	1 if multiple key indicators appear in a packet
11	8	Key-indicator-length	Byte length of the key indicator

3.7 Effects of Invention

The invention uses the tool list in IOD and IPMP Descriptors in OD to signal ISMACryp protection. By doing so, the signalling method can be made flexible, and can be truly compatible with the latest MPEG-4 IPMP Extension standard, hence makes the MPEG-system-capable ISMA receivers interoperable.

This invention also creates an ISMACryp_Data extending from IPMP_Data_BaseClass. The invented ISMACryp_Data can be used to carry the ISMACryp parameters, and subsequently be carried either in IPMP Descriptor or IPMP Stream. The carriage of ISMACryp parameters now become MPEG-4 IPMP Extension compliant.

4 BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows ISMACryp Architecture

Figure 2 shows the MPEG-4 IPMP Extension content structure.

Figure 3 shows the protection signaling using IPMP Descriptor

【書類名】　外国語図面

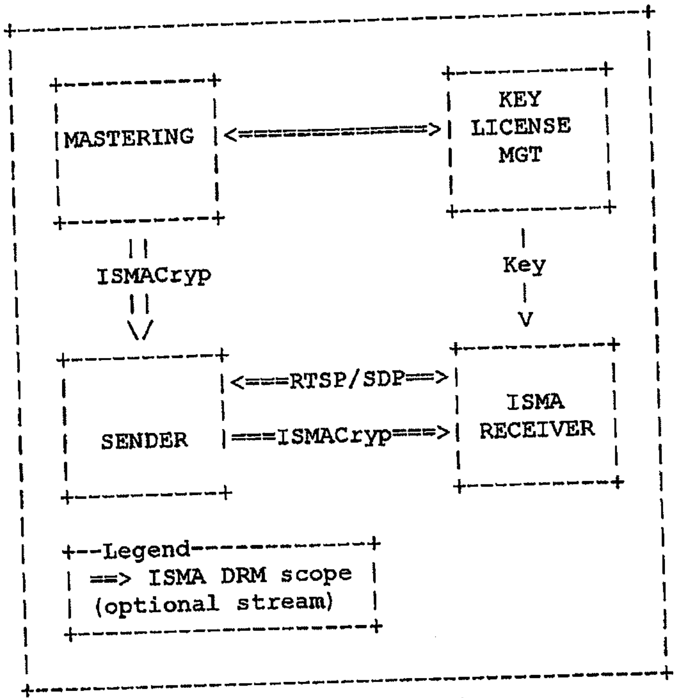

Figure 1: ISMACryp Architecture

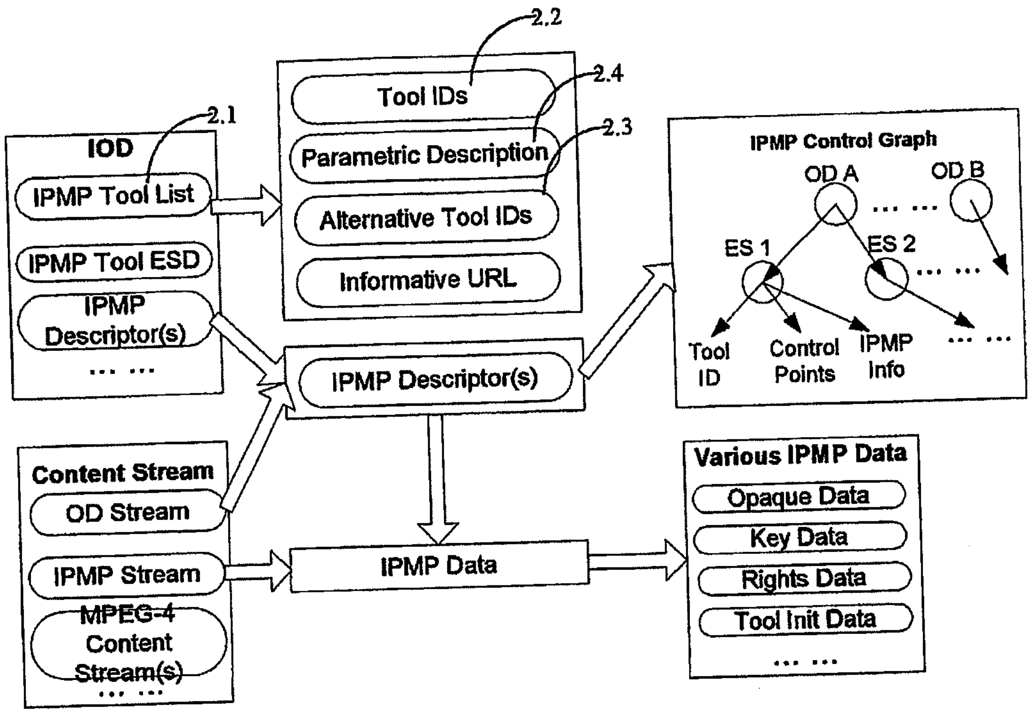

Figure 2: MPEG-4 IPMP Extension content structure.

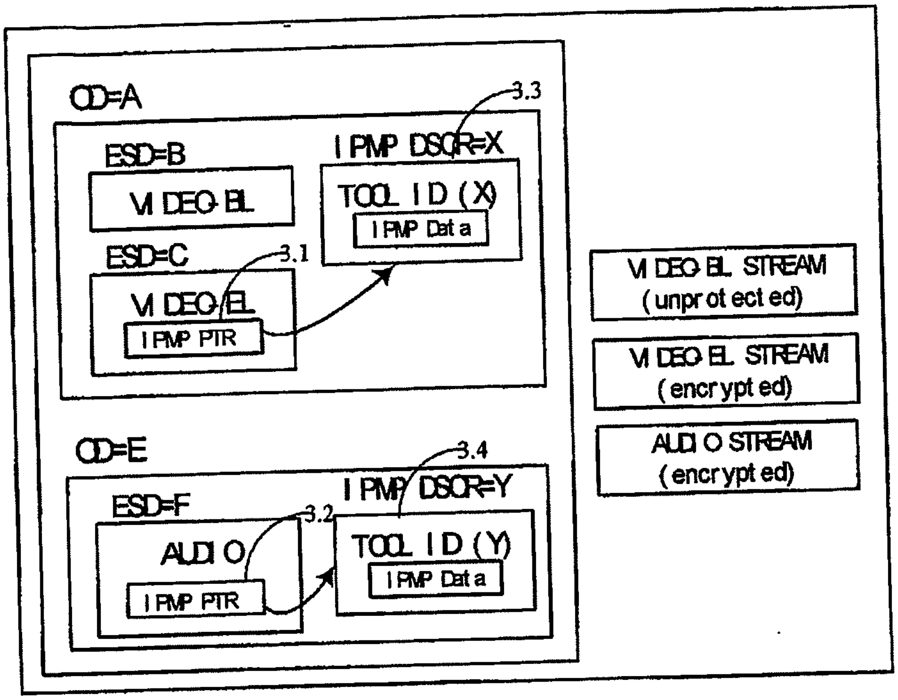

Figure 3: Protection signaling using IPMP Descriptor

【書類名】　外国語要約書

6 ABSTRACT

This invention defines a signalling mechanism to signal the presence of ISMACryp protection in MPEG Initial Object Descriptor (IOD). It utilizes the tool list and IPMP Descriptors to signal protection. This mechanism is compatible with the latest MPEG-4 IPMP Extension standard, to allow maximum interoperability with MPEG-system-capable ISMA receiver. It also provides a flexible way to identify tools required to play the content. (Fig. 1)

特願２００３－１３１３７２

出　願　人　履　歴　情　報

識別番号　　　　［０００００５８２１］

１．変更年月日　　１９９０年　８月２８日
　　［変更理由］　　新規登録
　　　住　所　　　大阪府門真市大字門真１００６番地
　　　氏　名　　　松下電器産業株式会社